

CLAIM AMENDMENTS

Claims 1-30 (canceled).

Claim 31 (currently amended): A computing system for securely accessing a first and a second ~~two separate~~ networks, comprising:

a central processing unit which is able to operate in a first and a second operation status;

~~a first and a second storage unit storing information of said first and said second operation status respectively wherein said information of said first and said second operation status is utilized by said central processing unit to execute computing operation in said first and said second operation status respectively~~ a first storage unit storing information of said first operation status wherein said information is utilized by said central processing unit to execute computing operation in said first operation status only;

a second storage unit storing information of said second operation status wherein said information is utilized by said central processing unit to execute computing operation in said second operation status only, wherein said first storage unit and said second storage unit are separated and said information of said first storage unit can not be accessed in said second operation status, said information of said second storage unit can not be accessed in said first operation status;

a first network adaptor which is communicatively connected with said first network in said first operation status only;

~~a first and a second network adaptor which is connected with a first network and a second network in said first and said second operation status respectively, wherein said two networks are physically separated~~ a second network adaptor which is communicatively connected with said second network in said second operation status only, wherein said first and second networks are physically separated, wherein said first network can not be connected in said second operation status, and said second network can not be connected in said first operation status; and

a switch device operatively communicated with said central processing unit to switch said operation status between said first and second operation status, wherein in said first operation status, said central processing unit is switched to access operation status information form said first storage unit, and said computing system is connected with said first network, wherein in said second operation status, said central processing unit is switched to access operation status information form said second storage unit, and said computing system is connected with said second network, wherein during the switching of operation status said central processing unit doesn't execute other computing operation.

Claim 32 (previously presented): The computing system, as recited in claim 31, wherein said switch device comprises a status switch command input unit adapted to trigger an input signal for switching between said first operation status and said second operation status; a secured switch control unit communicating with said command input unit and said central processing unit in such a manner that when said input signal is triggered, said secured switch control unit is adapted to generate a switch control signal which is then transmitted to said central processing unit for initialing a switching task between said first operation status and said second operation status; and a connection switch unit communicating with said secured switch control unit for switching connection between said first and second storage unit and said first and second network when said central processing unit is ready.

Claim 33 (previously presented): The computing system, as recited in claim 32, wherein during said switching process, said secured switch control unit prevents said central processing unit from performing other program and reacting to other interrupts.

Claim 34 (previously presented): The computing system, as recited in claim 33, wherein said secured switch control unit sends a non-maskable interrupt (NMI) to said central processing unit to execute operation status switching when said input signal is triggered.

Claim 35 (previously presented): The computing system, as recited in claim 32, wherein said secured switch control unit further comprises an identification verification unit which is adapted to verify an identify of a user giving said external switching command so as to ensure said switching between said first operation status and said second operation status is carried out by an authorized and legitimate user.

Claim 36 (previously presented): The computing system, as recited in claim 34, wherein said secured switch control unit further comprises an identification verification unit which is adapted to verify an identify of a user giving said external switching command so as to ensure said switching between said first operation status and said second operation status is carried out by an authorized and legitimate user.

Claim 37 (previously presented): The computing system, as recited in claim 35, wherein said first storage unit of said first operation status comprises a first random access memory module, a first display memory module, and a first hard disk, wherein said second storage unit of said second operation status comprises a second random access memory module, a second display memory module, and a second hard disk, wherein said connection of the central processing unit to said first random access memory module, first display memory module, and first hard disk, or to said second random access memory module, second display memory module, and second hard disk is switched by said connection switch unit.

Claim 38 (previously presented): The computing system, as recited in claim 36, wherein said first storage unit of said first operation status comprises a first random access memory module, a first display memory module, and a first hard disk, wherein said second storage unit of said second operation status comprises a second random access memory module, a second display memory module, and a second hard disk, wherein said connection of the central processing unit to said first random access memory module, first display memory module, and first hard disk, or to said second random access memory module, second display memory module, and second hard disk is switched by said connection switch unit.

Claim 39 (previously presented): The computing system, as recited in claim 32, wherein said secured switch control unit comprises a write-protect memory communicating with said central processing unit, wherein said write-protect memory stores the control commands for said central processing unit to perform operation status switching; and a monitoring unit adapted to receive said input signal for switching operation status from said command input unit, and interrupt said central processing unit to perform said control commands for operation status switching.

Claim 40 (previously presented): The computing system, as recited in claim 34, wherein said secured switch control unit comprises a write-protect memory

communicating with said central processing unit, wherein said write-protect memory stores the control commands for said central processing unit to perform operation status switching; a monitoring unit adapted to receive said input signal for switching operation status from said command input unit, and interrupt said central processing unit to perform said control commands for operation status switching.

Claim 41 (previously presented): The computing system, as recited in claim 36, wherein said secured switch control unit comprises a write-protect memory communicating with said central processing unit, wherein said write-protect memory stores the control commands for said central processing unit to perform operation status switching; a monitoring unit adapted to receive said input signal for switching operation status from said command input unit, and interrupt said central processing unit to perform said control commands for operation status switching.

Claim 42 (previously presented): The computing system, as recited in claim 38, wherein said secured switch control unit comprises a write-protect memory communicating with said central processing unit, wherein said write-protect memory stores the control commands for said central processing unit to perform operation status switching; a monitoring unit adapted to receive said input signal for switching operation status from said command input unit, and interrupt said central processing unit to perform said control commands for operation status switching.

Claim 43 (previously presented): The computing system, as recited in claim 39, further comprises a set trigger electrically connected to said monitoring unit for sending out a NMI signal to said central processing unit when switching operation status is allowed, and a reset trigger electrically connected to said monitoring unit and said set trigger in such a manner that when switching of said two operation statuses is finished, said monitoring unit is adapted to send a signal to said reset trigger, which then reset said set trigger and mask said switching function of said connection switch unit for preventing illegitimate switching between said two statuses.

Claim 44 (previously presented): The computing system, as recited in claim 40, further comprises a set trigger electrically connected to said monitoring unit for sending out a NMI signal to said central processing unit when switching operation status is allowed, and a reset trigger electrically connected to said monitoring unit and said set trigger in such a manner that when switching of said two operation statuses is finished,

said monitoring unit is adapted to send a signal to said reset trigger, which then reset said set trigger and mask said switching function of said connection switch unit for preventing illegitimate switching between said two statuses.

Claim 45 (previously presented): The computing system, as recited in claim 41, further comprises a set trigger electrically connected to said monitoring unit for sending out a NMI signal to said central processing unit when switching operation status is allowed, and a reset trigger electrically connected to said monitoring unit and said set trigger in such a manner that when switching of said two operation statuses is finished, said monitoring unit is adapted to send a signal to said reset trigger, which then reset said set trigger and mask said switching function of said connection switch unit for preventing illegitimate switching between said two statuses.

Claim 46 (previously presented): The computing system, as recited in claim 42, further comprises a set trigger electrically connected to said monitoring unit for sending out a NMI signal to said central processing unit when switching operation status is allowed, and a reset trigger electrically connected to said monitoring unit and said set trigger in such a manner that when switching of said two operation statuses is finished, said monitoring unit is adapted to send a signal to said reset trigger, which then reset said set trigger and mask said switching function of said connection switch unit for preventing illegitimate switching between said two statuses.

Claim 47 (previously presented): A method of securely switching at least two operation statuses to access at least two physically separated networks alternatively, wherein said method comprises the steps of:

- (a) receiving a request for switching said computing system from a first operation status to a second operation status by a command input unit;
- (b) analyzing said request for switching to determine whether to execute;
- (c) sending a non-maskable interrupt to said central processing unit to process operation status switching if said request switching is accepted;
- (d) saving information of said first operation status in a first storage unit;

- (e) connecting to a second storage unit;
- (f) connecting to a second network;
- (g) reading information of said second operation status;
- (h) processing requested function in said second operation status;
- (i) saving information of said second operation status;
- (j) connecting to said first storage unit;
- (k) connecting to said first network;
- (l) reading information of said first operation status; and
- (m) switching back to said first operation status.

Claim 48 (previously presented): The method, as recited in claim 47, wherein in step (b) further comprises a step of verifying an identification of a user executing said request for switching said computing system from said first operation status to said second operation status.

Claim 49 (previously presented): The method, as recited in claim 48, further comprises a step of masking a switching function during said switching of operation status, so as to minimize a possibility of said operation status being switched illegitimately.

Claim 50 (previously presented): The method, as recited in claim 49, further comprises a step of ensuring that said processing operation status switching is executed only by a prearranged control program so as to prohibit illegitimate switching of said operation status.